

**Prepared Statement by Senator Chuck Grassley of Iowa  
Chairman, Senate Judiciary Committee  
Joint hearing of the Senate Judiciary Committee and Senate Commerce Committee  
Facebook, Social Media Privacy, and the Use and Abuse of Data  
April 10, 2018**

The history and growth of Facebook mirrors that of many of our technology giants. Founded by Mr. Zuckerberg in 2004, Facebook has exploded over the last 14 years. Facebook currently has 2.13 billion monthly active users across the world, more than 25,000 employees, and offices in 13 U.S. cities and various other countries.

Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship status. Today, Facebook has access to dozens of data points, ranging from ads you've clicked on, events you've attended, and your location based on your mobile device.

It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated \$40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.

Significant data collection is also occurring at Google, Twitter, Apple, and Amazon. An ever-expanding portfolio of products and services offered by these companies grant endless opportunities to collect increasing amounts of information on their customers. As we get more free, or extremely low-cost, services, the tradeoff for the American consumer is to provide more personal data.

The potential for further growth and innovation based on the collection of data is limitless. However, the potential for abuse is significant.

While the contours of the Cambridge Analytica situation are still coming to light, there was clearly a breach of consumer trust and a likely improper transfer of data. The Judiciary Committee will hold a separate hearing exploring Cambridge and other data privacy issues.

More importantly though, these events have ignited a larger discussion on consumers' expectations and the future of data privacy in our society.

It has exposed that consumers may not fully understand or appreciate the extent to which their data is collected, protected, transferred, used and misused.

Data has been used in advertising and political campaigns for decades. The amount and types of data obtained, however, has seen a dramatic change. Campaigns, including President Bush, Obama, and Trump, all used these increasing amounts of data to focus on micro-targeting and personalization over numerous social media platforms, especially Facebook.

In fact, President Obama's campaign developed an app utilizing the same Facebook feature as Cambridge Analytica to capture the information of not just the app's users, but millions of their friends. The digital director for Obama for America 2012 described the data-scraping app as something that would "wind up being the most groundbreaking piece of technology developed for this campaign"

The effectiveness of these social media tactics can be debated, but their use over the past years across the political spectrum and their increased significance cannot.

Our policy towards data privacy and security must keep pace with these changes. Data privacy should be tethered to consumer needs and expectations.

At a minimum, consumers must have the transparency necessary to make informed decisions about whether to share their data and how it can be used. Consumers ought to have clear information, not opaque policies and complex click-through consent pages.

The tech industry has an obligation to respond to widespread and growing concerns over data privacy and security and to restore the public trust. The status quo no longer works.

Moreover, Congress must determine if and how we need to strengthen privacy standards to ensure transparency and understanding for the billions of consumers who utilize these products.